Development

This Briefing is Classified TOP SECRET//COMINT//ORCON//NOFORN

Tailored Access Operations

This Briefing is Classified TOP SECRET//COMINT//ORCON//NOFORN

DERIVED FROM: NSA/CSS Manual 1-52, Dated: 20070108, Declassify On: 20320108

TAO Mission

- **Sustain a deep, persistent, and pervasive presence on critical target networks**
- **Rapidly penetrate and track the communications of high-value individuals**
- **Continually execute CNE; support CNA and CND**
  - CNE: Exploit networks for foreign intelligence
  - CNA: Provide access and capabilities to support authorized network attacks
  - CND: Hunt foreign cyber actors on foreign networks
  - Deconflict DoD CNO with IC/Foreign partners
- **Build the techniques, tools and infrastructure required**
  - Subvert endpoint devices
    - Servers, workstations, firewalls, routers, handsets, phone switches, SCADA systems, etc.
  - Covertly communicate with implants in target networks
  - Automate CNE operations and maintenance of a large number of accesses

Aggressively Scale CNO Capabilities and Operations

TAO Organization

Requirements & Targeting

Manage ops requirements
Perform target development

Remote Operations Center

Conduct On-net ops (exploit, collect, geo-locate)

Data Network Technologies

Develop operational concepts and software implants to exploit computer networks

Telecommunications Network Technologies

Develop operational concepts and software implants to exploit phone switches
Develop network warfare capabilities
Network shaping

Access Technologies & Operations

Conduct physical access (off-net) operations
Conduct expeditionary CNO
Develop hardware and firmware implants to access isolated or complex networks

Mission Infrastructure Technologies

Design, development and delivery of the end-to end infrastructure that supports GENIE operations

Access Technology & Operations

- conducts global off-net operations with HUMINT partners to develop and deploy technology that enables on-net operations targeting high priority target networks and individuals.
- works closely with development organizations to create technical and operational solutions using specialized TAO hardware and software tools that are tailored to each mission and opportunity.
- bring unique talents to gaining access to intelligence when conventional collection methods prove ineffective.
- The diverse skill sets that ATO personnel bring to the mission leverages the support of our HUMINT partners, unique access, and sophisticated tools and techniques that provide physical access to networks and communications.

Access & Target Development

- (S//SI) Develop deep understanding of target communication techniques and practices of target entities with goal of identifying vulnerabilities that can be exploited via physical access.
- Define and develop physical access strategies, aligned to national requirements and TAO priorities, with emphasis on hard targets and isolated networks.
- Build and maintain significant relationships within the HUMINT community necessary for achieving access.
- Drive resulting operations to achieve end-to-end SIGINT successes.

Access Technology & Operations

Field Operations

(TS//SI//REL) The Field Operations Division is responsible for the developing and deploying customized SIGINT collection and data exfiltration solutions that enable remote network operations by gaining access to isolated target networks. The Division is also responsible for maintaining access to selected targets, exploring methods of enhancing the value from existing access, efficiently managing sustained operations, and working closely with the FBI and other HUMINT partners to plan and conduct operations.

Access and Target Development

- (S//SI) Develop deep understanding of target communication techniques and practices of target entities with goal of identifying vulnerabilities that can be exploited via physical access. Define and develop physical access strategies, aligned to national requirements and TAO priorities, with emphasis on hard targets and isolated networks. Build and maintain significant relationships within the HUMINT community necessary for achieving access. Drive resulting operations to achieve end-to-end SIGINT successes.

Expeditionary Access Operations (EAO)

(TS//SI//REL TO USA FVEY) S3283 is the expeditionary arm of TAO which conducts worldwide Human-Enabled Close Access Cyber Operations to satisfy National and Tactical SIGINT access requirements.

Persistence Divison

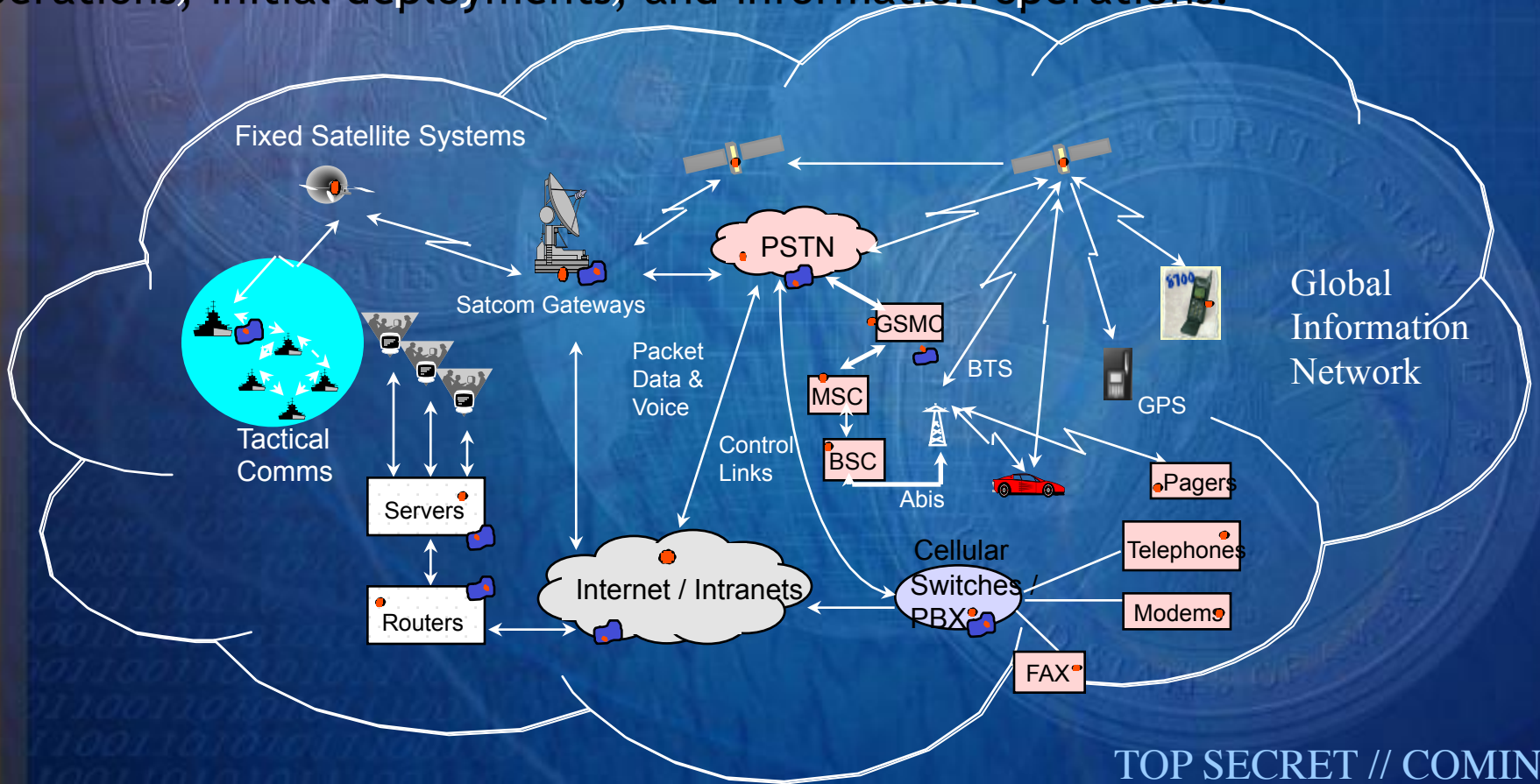
(U//FOUO) The Persistence Division (S3285) conceives, develops, tests, and integrates sophisticated firmware and software-based capabilities and techniques to directly support three of Tailored Access Operations' (TAO's) mission technology focus areas: **Persistence** - **IT/GEO** - **Computer Network Attack** (TS//SI//REL FVEY) These firmware and software techniques are remotely deployable to target devices via a network connection or by physical interdiction. Regardless of the deployment methodology, these highly developed accesses operate covertly without any indication of their presence and provide TAO with unique and advanced capabilities that directly support NSA and its other Intelligence Community partners with some of their most significant successes.

Telecom Network Technologies

- Providing logically intrusive methods of manipulating or extracting data from telecommunications networks.

TNT Mission:

"Define, design, develop, & test, logically intrusive methods of manipulating & extracting data from telecommunication networks, public infrastructures, and public broadcasting networks – and supporting enabling efforts, remote operations, initial deployments, and information operations."



Targeted Technologies:

- Telephony:
  - VOIP - Voice Over Internet Protocol
  - ISDN – Integrated Services Digital Network
  - GSM - Global Systems for Mobile Communications
  - GPRS – General Packet Radio Service
  - 3G – 3rd Generation Mobile Telephony
  - SMS – Short Messaging Service
  - MMS – Multimedia Messaging Service
  - SDH – Synchronous Digital Hierarchy
- Facilities & Infrastructure:
  - Data communications standards (ITU & IEEE)
- Broadcast:
  - ITU standards for digital video communications

CBND Overview

- Control Platforms Branch
  - Large Scale SCADA Energy Management Systems (EMSs)
  - Vendors
    - Siemens
    - Areva
    - ABB
- Control Devices Branch
  - Substation SCADA Technologies
  - Technologies
    - Programmable Logic Controllers (PLCs)
    - Intelligent Relays
- Video Technologies Branch
  - Video Teleconferencing Systems (VTCs)
  - Personal Video Technologies
    - Webcams
    - Internet Chat (Skype, etc)

Project Descriptions

- OPERATIONAL
  - GSM implants deployed in several target networks
  - Geolocation tools used with great success
  - Metadata and other voice collection tools
- DEVELOPMENT
  - GPRS and UMTS
- STRATEGIC EFFORTS
  - IP exfiltration
  - Enabling passive SIGINT collection

VND Overview

- Enterprise Telephony
  - Private Branch Exchanges (PBXs)
  - VoiceMail Systems
  - Network Management Systems
  - Technologies
    - SIP, H.323, SCCP
    - Linux & Windows development platforms
    - C, Assembly, Perl/Python
    - Ghidra, IDA Pro, JTAG for reverse engineering
- Transport Services
  - SDH, SONET Multiplexers
  - ATM Routers
  - Technologies
    - SDH, SONET, ATM
    - Linux & Windows development platforms
    - C, Assembly, Java
    - Ghidra, IDA Pro, JTAG for reverse engineering

Data Network Technologies

- Providing the software-based capabilities needed to surreptitiously exploit computer networks and the technology needed to covertly pass endpoint access commands and data across public networks to support endpoint operations.

Data Network Technologies

Access Division, S3231

(TS//SI) The Chief, Access Division is responsible to the Chief, Data Net-work Technologies Office to develop access to targets of interest to NSA. The Access Division focuses on developing remote access techniques and tools, ensuring continued remote access through the deployment of tools via remote or human assets, and assisting with remote access operations under the authority of the Remote Operations Center. The Access Division will act as the front door for DNT-wide efforts. The techniques developed should be scalable, automatable, and robust.

Network Technology Division, S3235

(S//SI//REL) The Chief, Network Technology Division is responsible to the Chief, Data Network Technologies Office for the development of tools and techniques to exploit components on global and private networks supporting endpoint operations.

Computer Technology Division, S3234

(TS//SI) The Chief, Computer Technology Division is responsible to the Chief, Data Networks Technologies Office for collection against target networks. The Computer Technology Division focuses on the development of software implants, automation, and control tools to support endpoint operations.

Cyber Networks Technology Division, S3232

(TS//SI) The Chief, Cyber Networks Technology Division (CNTD) is responsible to the Chief, Data Net-work Technologies Office to develop and deploy logically intrusive, software-based, end-point access techniques to enable Computer Network Operations (CNO) across multiple target operating systems and platforms. CNTD's purpose is to collect or enable collection of data for Foreign Intelligence and Operational Information and to include support to Information Operations.

Data Network Technologies

Cyber Network Technologies Division (CNTD)

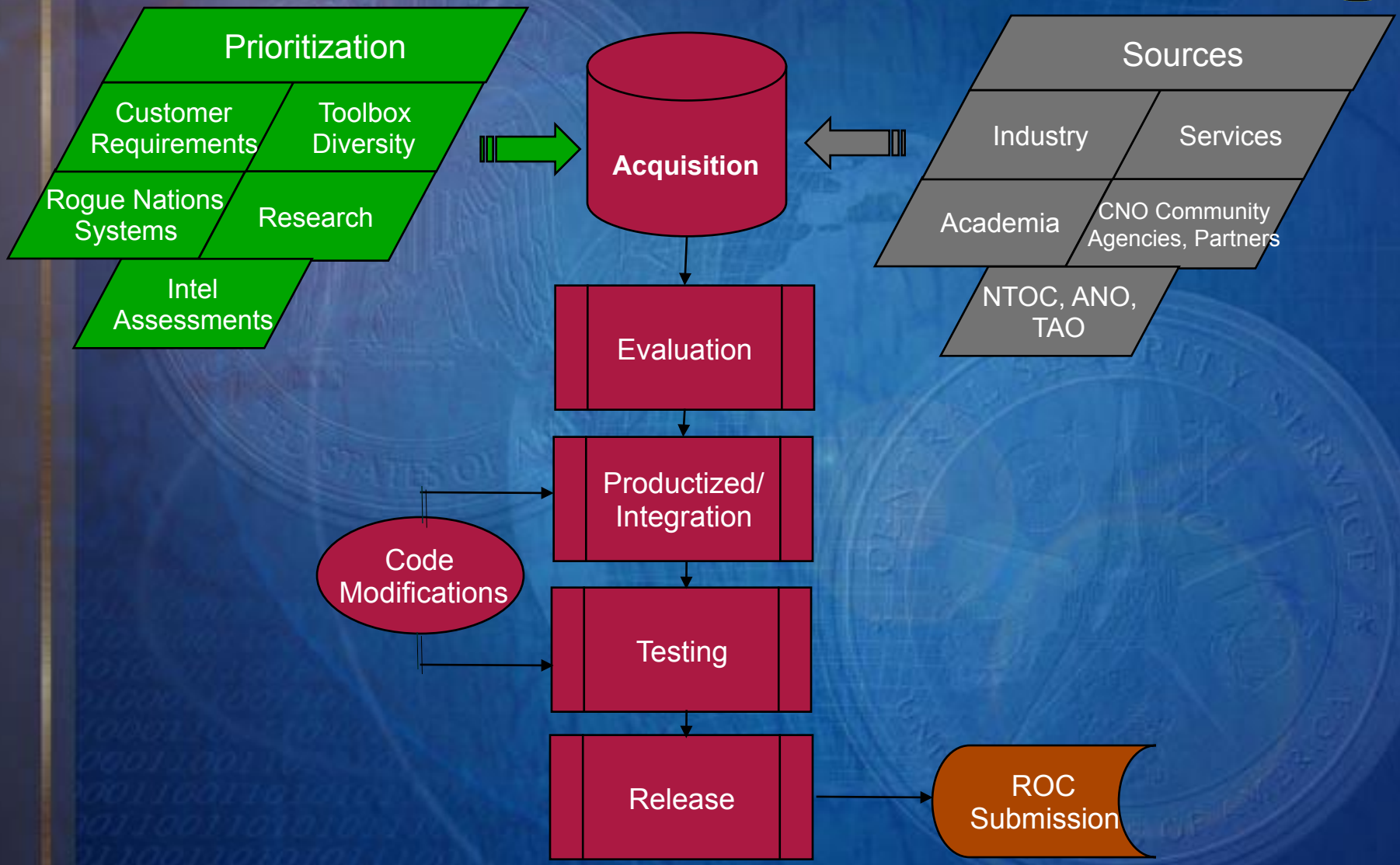
- Mission:
  - (TS//SI//NF) Develop and deploy logically intrusive, software-based, end-point access techniques to enable Computer Network Operations (CNO).
- Purpose:
  - (TS//SI//NF) Collect or enable collection of data for Foreign Intelligence and Operational Information, to include support to Information Operations.
- The Bottom Line
  - (TS//SI//NF) "Provide the War-fighter with a world class capability for computer network attacks and counter-computer network exploitations".
  - (TS//SI//NF) Develop mission applications that Deny, Destroy, Degrade, Disrupt, Manipulate, Mislead, and Collect against enemy targets.
  - (TS//SI//NF) Design and develop techniques that enable stealthy sustained operation of our mission applications on target.
  - (TS//SI//NF) Accomplish the above points across many target operating systems and platforms.

CNTD Overview

Acquisitions and Evaluations Branch (AEB)

- Search for or identify opportunities to purchase tools and their source code
- Validate, prioritize opportunities with appropriate development organization
- Acquire tools and their source code, provide in-depth evaluation to accurately assess the tools functionality
- Productize tools by modifying/developing for OPSEC, tradecraft, integration, testing with other TAO capabilities in order to meet operational requirements.

Methodology



CNTD Overview

Forensics and Engineering Branch (FEB)

- **Mission:**
  - (TS//SI//NF) Evaluate, Reverse Engineer, Exploit, and Repurpose software for use in CNE, CCNE and CNA operations.
- **Purpose:**
  - (TS//SI//NF) Reverse engineer and evaluate software from malware, nation-state, and commercial sources for the purpose of identifying tradecraft signatures and vulnerabilities.

Questions???